(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－47580
（P2000－47580A）
(43)公開日　平成12年２月18日(2000.2.18)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
G09C	1/00	610	G09C	1/00	610C
		660			660A
G08G	1/017		G08G	1/017	
H04L	9/06		H04L	9/00	611B

審査請求　未請求　請求項の数13　ＯＬ　（全 18 頁）

(21)出願番号　特願平11－119187
(22)出願日　平成11年４月27日(1999.4.27)
(31)優先権主張番号　特願平10－148712
(32)優先日　平成10年５月29日(1998.5.29)
(33)優先権主張国　日本（ＪＰ）

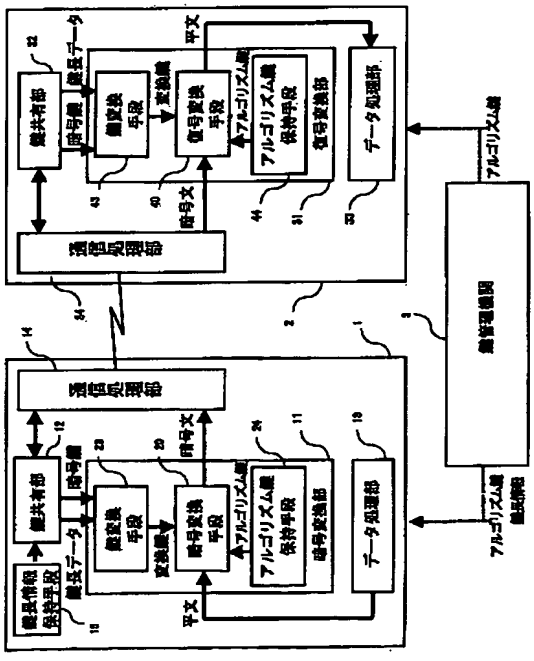
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　相川　慎
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(72)発明者　平畠　茂
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　暗号変換装置、復号変換装置、暗号通信装置および自動料金徴収装置

(57)【要約】　（修正有）
【課題】暗号変換のアルゴリズムを可変にし、アルゴリズムを第三者から隠すことで、暗号解読に強くする。
【解決手段】通信を行う送信機器と受信機器の間で、お互いに等しい暗号鍵を用いる。送信機器１が有する暗号変換手段の変換アルゴリズムは、送信機器が有する第１のアルゴリズム鍵保持手段に保持されている、第１のパラメータにより決定され、受信機器２が有する復号変換手段の変換アルゴリズムは、受信機器が有する第２のアルゴリズム鍵保持手段に保持されている、第２のパラメータにより決定される。送信機器と受信機器は、暗号鍵の他に、第１のパラメータと第２のパラメータが等しい場合のみ、送信機器が暗号鍵を用いて暗号化した暗号文を、受信機器が暗号鍵を用いて正しく復号化できる。

図１



1

【特許請求の範囲】

【請求項１】少なくとも１個の暗号鍵と、少なくとも１個のアルゴリズムパラメータと、平文データとを入力し、暗号文データを出力する暗号変換装置であって、

排他的論理和演算と、循環シフト演算と、加算演算とを各々少なくとも１回行う、暗号変換手段を複数段備え、

前記暗号変換手段は、入力データを、前記暗号鍵データから生成されるデータの一部と排他的論理和演算あるいは加算演算する、第１の演算手段と、

入力データを、前記アルゴリズムパラメータにより決定されるデータの一部と排他的論理和演算あるいは加算演算する、第２の演算手段と、

入力データを、前記アルゴリズムパラメータにより決定されるビット数だけ循環シフトする第３の演算手段を、各々少なくとも1個含み、

同一の前記暗号鍵と同一の前記アルゴリズムパラメータを用い、全ての前記暗号変換手段の中から任意に選んだ、連続した複数段の前記暗号変換手段を用いた変換は、全て異なっていることを特徴とする暗号変換装置。

【請求項２】少なくとも１個の暗号鍵と、少なくとも１個のアルゴリズムパラメータと、暗号文データとを入力し、平文データを出力する復号変換装置であって、

前記暗号変換手段は、入力データを、前記暗号鍵データから生成されるデータの一部と排他的論理和演算あるいは加算演算する、第１の演算手段と、

入力データを、前記アルゴリズムパラメータにより決定されるデータの一部と排他的論理和演算あるいは加算演算する、第２の演算手段と、

入力データを、前記アルゴリズムパラメータにより決定されるビット数だけ循環シフトする第３の演算手段とを、各々少なくとも1個含み、

同一の前記暗号鍵と同一の前記アルゴリズムパラメータを用い、全ての前記復号変換手段の中から任意に選んだ、連続した複数段の前記復号変換手段を用いた変換は、全て異なっていることを特徴とする復号変換装置。

【請求項３】通信を行う送信機器と受信機器の間で、お互いに等しい暗号鍵を用い、前記送信機器は平文を前記暗号鍵で暗号化して暗号文として送信し、前記受信機器は受信した前記暗号文を前記暗号鍵で復号化して前記平文を取得する共通鍵暗号を有する暗号通信装置であって、

前記送信機器は、暗号変換手段と、第１のアルゴリズム鍵保持手段を有し、

前記受信機器は、復号変換手段と、第２のアルゴリズム鍵保持手段を有し、

前記送信機器が有する前記暗号変換手段の変換アルゴリズムは、前記送信機器が有する前記第１のアルゴリズム鍵保持手段に保持されている、第１のパラメータにより決定され、

前記受信機器が有する前記復号変換手段の変換アルゴリズムは、前記受信機器が有する前記第２のアルゴリズム鍵保持手段に保持されている、第２のパラメータにより決定され、

前記送信機器と前記受信機器は、前記暗号鍵の他に、前記第１のパラメータと前記第２のパラメータが等しい場合のみ、前記送信機器が前記暗号鍵を用いて暗号化した前記暗号文を、前記受信機器が前記暗号鍵を用いて正しく復号化できることを特徴とする暗号通信装置。

【請求項４】請求項３記載において、前記送信機器は、あらかじめ定められた固有の第３のパラメータを前記第１のパラメータとして用い、前記受信機器は、前記第３のパラメータを前記第２のパラメータとして用いることを特徴とする暗号通信装置。

【請求項５】通信を行う送信機器と受信機器の間で、お互いに等しい暗号鍵を用い、前記送信機器は平文を前記暗号鍵で暗号化して暗号文として送信し、前記受信機器は受信した前記暗号文を前記暗号鍵で復号化して前記平文を取得する共通鍵暗号を有する暗号通信装置であって、

前記送信機器は、鍵長保持手段と、第１の鍵共有手段と、暗号変換手段とを有し、

前記受信機器は、第２の鍵共有手段と、復号変換手段とを有し、

前記送信機器と前記受信機器は、暗号通信を開始する前に、前記送信機器が有する前記鍵長保持手段に保持されている鍵長データを基に、前記送信機器が有する前記第１の鍵共有手段と、前記受信機器が有する前記第２の鍵共有手段を用いて、前記鍵長データで指定された長さの前記暗号鍵を共有することを特徴とする暗号通信装置。

【請求項６】請求項５記載において、前記送信機器は、あらかじめ定められた固有の鍵長データを用いることを特徴とする暗号通信装置。

【請求項７】請求項５記載において、前記暗号変換手段は、換字転置混合変換を行う第１の換字転置変換手段を複数段備え、前記暗号鍵あるいは前記暗号鍵を変換したデータを用いて、前記平文を、各々の前記第１の換字転置変換手段に作用させることで、前記暗号文を出力するものであって、

前記第１の換字転置変換手段におけるデータ変換は、ビット列変換手段を含み、前記ビット列変換手段は複数段の循環シフト演算手段と、複数段の加算演算手段とを含むことを特徴とする暗号変換装置。

【請求項８】請求項７記載において、前記循環シフト演算手段の各々の出力結果は、入力される変換データと前記第３のパラメータの一部により決定されることを特徴とする暗号変換装置。

【請求項９】請求項７記載において、前記加算演算手段の各々の出力結果は、入力される変換データと前記第３のパラメータの一部により決定されることを特徴とする暗号変換装置。

【請求項１０】請求項５記載において、前記復号変換手段は、換字転置混合変換を行う第２の換字転置変換手段を複数段備え、前記暗号鍵あるいは前記暗号鍵を変換したデータを用いて、前記暗号文を、前記第２の換字転置変換手段の各々に作用させることで、前記平文を出力するものであって、

前記第２の換字転置変換手段におけるデータ変換は、請求項５に記載の前記ビット列変換手段により実行されることを特徴とする復号変換装置。

【請求項１１】ＩＣカードを挿入している車載機を搭載した自動車が、有料道路の路側機を通過する際に、自動車を停止することなく、通行料金を徴収できる、自動料金徴収装置であって、前記車載機は、前記暗号復号変換手段に加えて、第１のアルゴリズム鍵保持手段を有すると共に、前記車載機が有する前記暗号復号変換手段の変換アルゴリズムは、前記車載機が有する前記第１のアルゴリズム鍵保持手段に保持されている、第１のパラメータにより決定される、前記自動料金徴収装置、において用いられる前記ＩＣカードであって、

前記ＩＣカードは、前記暗号復号変換手段に加えて、第２のアルゴリズム鍵保持手段を有し、前記ＩＣカードが有する前記暗号復号変換手段の変換アルゴリズムは、前記ＩＣカードが有する前記第２のアルゴリズム鍵保持手段に保持されている、第２のパラメータにより決定され、

前記第２のパラメータが前記第１のパラメータと等しい場合のみ、前記車載機と暗号通信が行えることを特徴とするＩＣカード。

【請求項１２】ＩＣカードを挿入している車載機を搭載した自動車が、有料道路の路側機を通過する際に、自動車を停止することなく、通行料金を徴収できる、自動料金徴収装置であって、前記路側機は、前記暗号復号変換手段に加えて、第１のアルゴリズム鍵保持手段を有すると共に、前記路側機が有する前記暗号復号変換手段の変換アルゴリズムは、前記路側機が有する前記第１のアルゴリズム鍵保持手段に保持されている、第１のパラメータにより決定される、前記自動料金徴収装置、において用いられる前記車載機であって、

前記車載機は、前記暗号復号変換手段に加えて、第２のアルゴリズム鍵保持手段を有し、前記車載機が有する前記暗号復号変換手段の変換アルゴリズムは、前記車載機が有する前記第２のアルゴリズム鍵保持手段に保持されている、第２のパラメータにより決定され、

前記第２のパラメータが前記第１のパラメータと等しい場合のみ、前記路側機と暗号通信が行えることを特徴とする車載機。

【請求項１３】ＩＣカードを挿入している車載機を搭載した自動車が、有料道路の路側機を通過する際に、自動車を停止することなく、通行料金を徴収できる、自動料金徴収装置であって、前記車載機は、前記暗号復号変換

手段に加えて、第１のアルゴリズム鍵保持手段を有すると共に、前記車載機が有する前記暗号復号変換手段の変換アルゴリズムは、前記車載機が有する前記第１のアルゴリズム鍵保持手段に保持されている、第１のパラメータにより決定される、前記自動料金徴収装置、において用いられる前記路側機であって、

前記路側機は、前記暗号復号変換手段に加えて、第２のアルゴリズム鍵保持手段を有し、前記路側機が有する前記暗号復号変換手段の変換アルゴリズムは、前記路側機が有する前記第２のアルゴリズム鍵保持手段に保持されている、第２のパラメータにより決定され、

前記第２のパラメータが前記第１のパラメータと等しい場合のみ、前記車載機と暗号通信が行えることを特徴とする路側機。

【発明の詳細な説明】

【発明の属する技術分野】本発明は、コンピュータ、情報家電機器、自動料金徴収装置等の間で伝送されるデジタル・データの暗号・復号技術に関するものである。

【従来の技術】一般に、デジタル情報家電機器においては、デジタルデータの不正な複写を防ぐための暗号化技術が必須となる。たとえば、デジタル放送受信機で受信したデジタル映像データを、デジタル録画機器にデジタル録画する場合、デジタル映像データに著作権があれば、それを保護する機能がそれぞれの装置に必要になる。このような著作権保護システムを実現するためには、デジタルデータの複写制限の設定、機器間認証、デジタルデータのリアルタイム暗号化などの暗号技術を用い、データの改ざんや不正な複写を防止しなければならない。暗号技術の従来例としては、例えば日本特開昭51-108701号公報に示されるＤＥＳ暗号に代表される、共通鍵暗号方式が挙げられる。共通鍵暗号方式の多くは、簡単な変換を繰り返し行うことで、複雑な暗号変換を構成することを特徴としている。これらの暗号をより安全なものにする工夫は従来から様々な形でなされてきた。例えば、簡単な変換の繰り返し回数を大きくすることで、暗号文の統計的な特徴をより撹乱し、暗号解読を困難にできる。

【発明が解決しようとする課題】しかし、変換の繰り返し回数を増やすことは、暗号変換に要する処理時間を増大してしまうことになる。したがって、簡単な変換の繰り返し回数を大きくすることによる安全性強化対策は、上述した著作権保護システムにおける、リアルタイム暗号化処理には適さないという問題があった。本発明の目的は、暗号変換のアルゴリズムを可変にし、使用するアルゴリズムを第三者から隠すことで、暗号解読に強い、高速な暗号変換装置、復号変換装置、暗号通信装置および自動料金徴収装置を提供することにある。

【課題を解決するための手段】暗号変換装置としては、少なくとも１個の暗号鍵と、少なくとも１個のアルゴリズムパラメータと、平文データとを入力し、暗号文デー

タを出力する暗号変換装置であって、排他的論理和演算と、循環シフト演算と、加算演算とを各々少なくとも１回行う、暗号変換手段を複数段備え、前記暗号変換手段は、入力データを、前記暗号鍵データから生成されるデータの一部と排他的論理和演算あるいは加算演算する、第１の演算手段と、入力データを、前記アルゴリズムパラメータにより決定されるデータの一部と排他的論理和演算あるいは加算演算する、第２の演算手段と、入力データを、前記アルゴリズムパラメータにより決定されるビット数だけ循環シフトする第３の演算手段を、各々少なくとも1個含み、同一の前記暗号鍵と同一の前記アルゴリズムパラメータを用い、全ての前記暗号変換手段の中から任意に選んだ、連続した複数段の前記暗号変換手段を用いた変換は、全て異なっていることを特徴とする。復号変換装置としては、少なくとも１個の暗号鍵と、少なくとも１個のアルゴリズムパラメータと、暗号文データとを入力し、平文データを出力する復号変換装置であって、前記暗号変換手段は、入力データを、前記暗号鍵データから生成されるデータの一部と排他的論理和演算あるいは加算演算する、第１の演算手段と、入力データを、前記アルゴリズムパラメータにより決定されるデータの一部と排他的論理和演算あるいは加算演算する、第２の演算手段と、入力データを、前記アルゴリズムパラメータにより決定されるビット数だけ循環シフトする第３の演算手段とを、各々少なくとも1個含み、同一の前記暗号鍵と同一の前記アルゴリズムパラメータを用い、全ての前記復号変換手段の中から任意に選んだ、連続した複数段の前記復号変換手段を用いた変換は、全て異なっていることを特徴とする。暗号通信装置としては、通信を行う送信機器と受信機器の間で、お互いに等しい暗号鍵を用い、前記送信機器は平文を前記暗号鍵で暗号化して暗号文として送信し、前記受信機器は受信した前記暗号文を前記暗号鍵で復号化して前記平文を取得する共通鍵暗号を有する暗号通信装置であって、前記送信機器は、暗号変換手段と、第１のアルゴリズム鍵保持手段を有し、前記受信機器は、復号変換手段と、第２のアルゴリズム鍵保持手段を有し、前記送信機器が有する前記暗号変換手段の変換アルゴリズムは、前記送信機器が有する前記第１のアルゴリズム鍵保持手段に保持されている、第１のパラメータにより決定され、前記受信機器が有する前記復号変換手段の変換アルゴリズムは、前記受信機器が有する前記第２のアルゴリズム鍵保持手段に保持されている、第２のパラメータにより決定され、前記送信機器と前記受信機器は、前記暗号鍵の他に、前記第１のパラメータと前記第２のパラメータが等しい場合のみ、前記送信機器が前記暗号鍵を用いて暗号化した前記暗号文を、前記受信機器が前記暗号鍵を用いて正しく復号化できることを特徴とする。

【発明の実施の形態】以下、本発明の実施の形態を図面を用いて説明する。図１は、本発明による暗号変換装置を備えたデータ送信機器と、本発明による復号変換装置を備えたデータ受信機器とが暗号通信を行う暗号通信装置の構成図である。図１において、データ送信機器1は、暗号変換部11と、鍵共有部12と、データ処理部13と、通信処理部14と、鍵長データ保持手段15を備える。また、データ受信機器2は、復号変換部31と、鍵共有部32と、データ処理部33と、通信処理部34を備える。データ送信機器1は例えばデジタル放送受信機が考えられる。また、データ受信機器2は例えばデジタル録画機器が考えられる。この場合、データ処理部13および33は、デジタル放送サービスが配信するMPEG2-TS (Transport Stream)形式のようなデジタル番組データを扱うこととなり、データ処理部13は、デジタル番組データの受信処理、多重分離処理、伸長処理、送信処理などを行い、データ処理部33はデジタル番組データの受信処理、伸長処理、蓄積処理などを行う。データ送信機器1と、データ受信機器2が暗号通信を行う場合、まず、データを暗号化および復号化するために必要な暗号鍵と呼ばれるデータを共有する。暗号鍵の共有は、データ送信機器1の鍵共有部12と、データ受信機器2の鍵共有部32が、通信処理部14および通信処理部34を介し、メッセージを交換し合うことで行われる。この時、データ送信機器1の鍵長情報保持手段15に保持されている鍵長データを基に、暗号鍵の鍵長を決定する。二者間で共有する暗号鍵は、毎回異なっているのが望ましい。暗号鍵が異なれば生成される暗号文が異なるので、第三者による暗号文の解読攻撃を困難にできるからである。暗号鍵の共有の方法は様々な方法が考えられるが、例えば、デフィー・ヘルマンの鍵共有方法（例えば、岡本龍明他著,「現代暗号」,産業図書株式会社発行 の特に第２００頁乃至第２０２頁に詳しく記載されている）を用いる。これを用いれば、暗号鍵の共有のために交換するメッセージを第三者が盗聴しても、それらから暗号鍵を推定することが非常に困難であり、毎回異なった暗号鍵を安全に共有することが可能になる。データ鍵の共有後、データ送信機器1は、データ処理部13が送信したいデータを出力し、これを暗号変換部11に入力する。ここで、データ処理部13から出力されるデータは暗号化されてなく、このようなデータを以下「平文」と呼ぶことにする。暗号変換部11は、暗号変換手段20と、鍵変換手段23と、アルゴリズム鍵保持手段24から成る。鍵変換手段23は、暗号鍵と鍵長データを基に変換鍵と呼ばれる複数のデータを生成する。ここで、鍵長データは、上述した暗号鍵共有の際に決定した暗号鍵の鍵長を表す。アルゴリズム鍵保持手段24はアルゴリズム鍵と呼ばれる複数のデータを保持している。暗号変換手段20が行う暗号変換アルゴリズムはアルゴリズム鍵により決定される。暗号変換手段20は、鍵変換手段23で生成した変換鍵と、アルゴリズム鍵保持手段24内のアルゴリズム鍵とを用いて、平文を暗号変換し、暗号文を出力する。暗号変換装置11で生成された暗

号文は、通信処理部14でデータ受信機器2に送信される。データ受信装置2は、通信処理部34で暗号文を受信し、受信した暗号文を復号変換部31に入力する。復号変換部31は、復号変換手段40と、鍵変換手段43と、アルゴリズム鍵保持手段44から成る。鍵変換手段43は、前述した鍵変換手段23と同様の構成であり、暗号鍵と、鍵長データを基に変換鍵を生成する。また、アルゴリズム鍵保持手段44は、前述したアルゴリズム鍵保持手段24と同様の構成であり、アルゴリズム鍵を保持している。復号変換手段40が行う復号変換アルゴリズムはアルゴリズム鍵により決定される。復号変換手段40は、暗号文を、鍵変換手段43で生成した変換鍵と、アルゴリズム鍵保持手段44内のアルゴリズム鍵とを用いて、復号変換する。ここで復号変換手段40は、前述した暗号変換手段20と、同一のアルゴリズム鍵を用いた場合のみ、暗号変換手段20で暗号変換した暗号文を、復号変換手段40で元の平文に復号変換することが可能になる。復号変換部31から出力された平文は、データ処理部33に入力され、データ処理が行われる。以上説明したように、データ送信装置1とデータ受信装置2は、同一のアルゴリズム鍵を保持した場合のみ、暗号通信を行うことが可能になる。このアルゴリズム鍵を秘密情報として扱うことで、認証機能を有する暗号通信を実現することができる。すなわち、正当な機器のみが正しいアルゴリズム鍵を保持している構成にすれば、通信相手が正当な機器の場合のみ、暗号通信を行うことができる。これを実現するために、アルゴリズム鍵を生成して集中管理する鍵管理機関3を設けた例を図１に同時に示す。図１に示すように、正当な機器（ここでは、データ送信機器1とデータ受信機器2）は、鍵管理機関3からアルゴリズム鍵を外部に漏れないように安全に取得する。例えば、データ送信機器1およびデータ受信機器2の製造時に、鍵管理機関3が管理しているアルゴリズム鍵を、アルゴリズム鍵保持手段24およびアルゴリズム鍵保持手段44に埋め込んでおくことが考えられる。この時、データ受信機器1は、鍵長データも同時に取得しておく。これによって、正しいアルゴリズム鍵を保持している正当な機器が送信する暗号文は、正しいアルゴリズム鍵を保持している正当な機器しか復号化することができない。また、暗号鍵に加えて、アルゴリズム鍵も秘密情報であるので、第三者による通信路上を流れる暗号文の解読攻撃をより困難にすることができる。また、データ送信機1は、鍵長データを鍵管理機関3から取得し、これを基に暗号鍵を生成するので、暗号鍵の鍵長の更新が可能になる。例えば新規に製造するデータ送信機器に、更新した鍵長データを埋め込んでおけば、新規に製造されたデータ送信機器との暗号通信においては、暗号鍵の鍵長が更新できる。これによって、将来において暗号鍵の鍵長を長くし、より安全性を向上することができる。また、製品を出荷する地域によって鍵長を変更することができる。図２は、暗号変換部11の詳細なブロック図の一例を示す。ここで、暗号変換部11には、64ビットの平文と、40ビットあるいは64ビットの暗号鍵と、1ビットの鍵長データとが入力され、64ビットの暗号文が出力される。暗号鍵は、鍵鍵変換手段23で鍵長データを基に32ビットの変換鍵K1とK2に変換される。鍵長データは暗号鍵が40ビットならば0、64ビットならば1とする。鍵変換手段23の変換については後述する。暗号変換部11内の暗号変換手段20は、211から21Nの N個の換字転置変換手段から構成される。換字転置変換手段21n（ここで、1≦n≦N）の変換アルゴリズムは、アルゴリズム鍵保持手段24に保持されているアルゴリズム鍵Gnにより決定される。平文は、まず、上位32ビット値R0と下位32ビット値L0に分離されて、換字転置変換手段211に入力され、K1およびK2を用いて、１回目の暗号変換が行われ、32ビット値R1と32ビット値L1が出力される。続いて、R1とL1は換字転置変換手段212に入力され、 K1およびK2を用いて、２回目の暗号変換が行われ、32ビット値R2と32ビット値L2が出力される。以上のような暗号変換をN回繰り返し、最終的な出力値である32ビット値RNと32ビット値LNを結合することで、64ビットの暗号文を得る。ここで、 暗号変換の総繰り返し数Nをラウンド数と呼ぶものとする。ここで、暗号鍵を固定しておき、全ての換字転置変換手段から、連続する２個以上の換字転置変換手段を任意に選んで、同一のデータを入力値として変換することを考える。この場合、変換結果は、アルゴリズム鍵Gnにより決定される。本発明に基づいた暗号変換装置は、上述した全ての組み合わせにおいて、異なった変換結果がえられるようなアルゴリズム鍵のみを用いるものとする。すなわち、換字転置変換手段を繰り返し用いた暗号変換には周期性が現れない。これによって、暗号の強度を向上することができる。図３は、図２の鍵変換手段23のブロック図の一例を示す。図３において、鍵変換手段23は、64ビット長のレジスタ26と、マルチプレクサ27と、加算演算部28から成る。暗号鍵は、まずレジスタ26に格納される。ここで、暗号鍵が40ビットならば、レジスタ26の下位40ビットに値が格納され、暗号鍵が64ビットならば、レジスタ26の全てに値が格納される。次に、レジスタ26の下位32ビットをK1とする。次に、鍵長データの値が0ならば、レジスタ26の下位9ビット目から下位40ビット目までの32ビットの値がマルチプレクサ27の出力値として選ばれる。また、鍵長データの値が1ならば、レジスタ26の上位32ビットの値が、マルチプレクサ27の出力値として選ばれる。マルチプレクサ27の出力値は、加算演算部28で、K1と32ビット加算が行われ、この結果をK2とする。ここで32ビット加算とは、通常の加算結果を２の32乗で割った余りとするものである。図４は、図２において、n回目（ここで、1≦n≦N）の暗号変換を実行する換字転置変換手段21nのブロック図を示している。図４において、換字転置変換手段21nは、ビット列変換部61と、加算演算部62から構成され、 Rn-1とL

n-1を、K1とK2を用いて、 RnとLnに変換する。換字転置変換手段21nは、まず、Ln-1の値を、ビット列変換部61に入力する。ビット列変換部61は、アルゴリズム鍵Gnにより変換アルゴリズムが決定される。ビット列変換部61の入力値をU、出力値をZとすれば、数式で以下のように表すことができる。

Z = FGn (K1 , K2 ,U)

ここで、関数FGn(X)は、ビット列変換部61の変換を表す。また、アルゴリズム鍵Gnは、以下に示すデータからなる。

Gn = (An, Bn, Cn, Pn, Qn, Sn)

ここで、An, Bn, Cnは32ビットデータであり、Pn, Qn, Snは1≦Pn≦31, 1≦Qn≦31, 1≦Sn≦31である。アルゴリズム鍵Gnの値は、それぞれのn（1≦n≦N）で異なる値を取ってもよい。次に、Rn-1を、加算演算部32に入力し、Zn との62ビット加算演算を取り、Lnとする。最後に、 Ln-1の値をRnとする。以上の変換をまとめると、以下のように表せる。

Ln = Rn + FGn (K1 , K2 ,Ln-1)

Rn = Ln-1

図５は、図４のビット列変換部61のブロック図の一例を示す。ビット列変換部61は、５個のビット列変換器81から85で構成される。ビット列変換器81は、排他的論理和部94を備える。ビット列変換器82は、加算演算部95と循環シフト部91を備える。ビット列変換器83は、加算演算部96と循環シフト部92を備える。ビット列変換器84は、加算演算部97を備える。ビット列変換器85は、加算演算部98と循環シフト部93を備える。ビット列変換器81内の排他的論理和部94は、２個の入力値の排他的論理和演算を行う。２個の入力値の内、一つが図４に図示のK1であり、もう一つが図４に図示のU即ちビット列変換部61およびビット列変換器81の入力値である。ここで、出力値をVとすれば、ビット列変換器81の変換は、以下のように表せる。

V = K1(+)U

ここで、表記 X(+)YはXとYとの排他的論理和演算を示す。ビット列変換器82内の循環シフト部91は、アルゴリズム鍵Gnの一部であるデータPn（1≦Pn≦31）だけ左に循環シフトする。また、加算演算部95は３個の入力値の32ビット加算演算を行う。３個の入力値の内の一つが図４に図示のアルゴリズム鍵Gnの一部であるデータAnであり、もう一つがビット列変換器82の入力値Vであり、さらにもう一つが前述左に循環シフトのデータPn である。ここで、出力値をWとすれば、ビット列変換器82の変換は、以下のように表せる。

W = V + (V <<<Pn) + An

ここで、表記 X<<<Y は、Xを左にYビット循環シフトすることを表す。ビット列変換器83内の循環シフト部92は、アルゴリズム鍵Gnの一部であるデータQn（1≦Qn≦31）だけ左に循環シフトする。また、加算演算部96は３個の入力値の32ビット加算演算を行う。３個の入力値の内、一つが図４に図示のアルゴリズム鍵Gnの一部であるデータBnでであり、もう一つがビット列変換関器83の入力値Wであり、さらにもう一つが前述左に循環シフトのデータPn である。ここで、出力値をXとすれば、ビット列変換器83の変換は、以下のように表せる。

X = W + (W <<<Qn) + Bn

ビット列変換器84内の加算演算部97は、２個の入力値の32ビット加算演算を行う。２個の入力値の内、一つが図４に図示のK2であり、もう一つがビット列変換器84の入力値Xである。ここで、出力値をYとすれば、ビット列変換器84の変換は、以下のように表せる。

Y = K2 + X

ビット列変換器85内の循環シフト部93は、アルゴリズム鍵Gnの一部であるデータSn（1≦Sn≦31）だけ左に循環シフトする。また、加算演算部98は３個の入力値の32ビット加算演算を行う。３個の入力値の内、一つが図４に図示のアルゴリズム鍵Gnの一部であるデータCn であり、もう一つがビット列変換器85の入力値Yであり、さらにもう一つが前述左に循環シフトのデータSn である。ここで、出力値をZとすれば、ビット列変換器85の変換は、以下のように表せる。

Z = Y + (Y <<<Sn) + Cn

以上説明したように、ビット列変換部61は、５つのビット列変換器 81から 85を変換データに作用させていくことで、ビット列変換を行う。ここで、ビット列変換部61は、５つのビット列変換器 81から 85の変換データへの作用順序を変更した構成でも、本発明の範囲に含まれる。図３では、

F1 81 → F2 82 → F3 83 → F4 84 → F5 85

の順になっているが、例えばこれを、

F4 84 → F3 83 → F1 81 → F5 85 → F２ ８２

としてもよい。また、５個のビット列変換器 ８１から 85は、１個の排他的論理和部と、３個の循環シフト部と、４個の加算演算部から構成されるに限らず、換字転置混合変換が実現できる少なくとも１個の加算演算部と、少なくとも一個の循環シフト演算部とを含む構成としても、発明の効果は変らない。図６は、図１の復号変換部31の詳細なブロック図を示す。この復号変換部31は、前述した図２の暗号変換部11を用いて暗号変換した暗号文を、元のデータに復号するものである。復号変換部31には、64ビットの暗号文と、40ビットあるいは64ビットのデータ鍵と、1ビットの鍵長データが入力され、64ビットの平文が出力される。復号変換部31内の暗号変換手段40は、411から41NのN個の換字転置変換手段から構成される。換字転置変換手段41n（ここで、1≦n≦N）の変換アルゴリズムは、アルゴリズム鍵保持手段44に保持されているアルゴリズム鍵Gnにより決定される。暗号文は、まず、上位32ビット値RNと下位32ビット値LNに分離されて、換字転置変換手段41Nに入力され、K1およびK

2を用いて、１回目の復号変換が行われ、32ビット値RN-1と32ビット値LN-1が出力される。続いて、RN-1とLN-1は換字転置変換手段21N-1に入力され、 K1およびK2を用いて、２回目の暗号変換が行われ、32ビット値RN-2と32ビット値LN-2が出力される。以上のような復号変換をN回繰り返し、最終的な出力値である32ビット値R 0と32ビット値L0を結合することで、64ビットの平文を得る。ここで、復号変換の総繰り返し数Nを、暗号変換の場合と同様に、ラウンド数と呼ぶものとする。ここで、暗号鍵を固定しておき、全ての換字転置変換手段から、連続する２個以上の換字転置変換手段を任意に選んで、同一のデータを入力値として変換することを考える。この場合、変換結果は、アルゴリズム鍵Gnにより決定される。本発明に基づいた復号変換装置は、上述した全ての組み合わせにおいて、異なった変換結果がえられるようなアルゴリズム鍵のみを用いるものとする。すなわち、換字転置変換手段を繰り返し用いた復号変換には周期性が現れない。図７は、図６において、 (N+1-n)回目 (1≦n≦N) の復号変換を実行する換字転置変換手段41nのブロック図を示している。図７において、換字転置変換手段41nは、図５を用いて説明したビット列変換部61と、減算演算部72から構成され、ＲｎとＬｎを、K1とK2を用いて、Rn-1とLn-1に変換する。換字転置変換手段41nは、まず、Rnの値を、ビット列変換部61に入力する。ビット列変換部61は、アルゴリズム鍵Gnにより変換アルゴリズムが決定される。ここで、ビット列変換部31nの入力値をU、出力値をZと表す。次に、Lnを、減算演算部72に入力し、Z との32ビット減算演算を取り、Rn-1とする。ここで32ビット減算とは、通常の減算を行い、結果が負ならば、その値を２の32乗と加算するものである。最後に、 Rnの値をLn-1とする。以上の変換をまとめると、以下のように表せる。

Rn-1 = Ln - FGn (K1 , K2 ,Rn)

Ln-1 = Rn

この変換は、図２を用いて説明した、換字転置変換手段21nの逆変換を行う。これによって、復号変換部31は、暗号変換部11との間で、同じ暗号鍵およびアルゴリズム鍵を共有すれば、暗号変換部11が暗号化したデータを復号化することができる。以上、図１から図７を用いて、本発明による暗号変換部を備えたデータ送信機器1と、本発明による復号変換部を備えたデータ受信機器2の実施例を詳細に説明した。しかしながら、上記の構成の一部を変更した構成も本発明に含まれることは明らかである。例えば、暗号鍵を40ビットと64ビットの２つの例で、鍵長データを1ビットとして説明したが、これに限るものではない。例えば、暗号鍵を40ビットから128ビットまで変更可能とし、鍵長データはこれらを選択できるように7ビットとしても良い。この場合、鍵変換手段では、２個の32ビット長である変換鍵を生成できるように、入力された鍵長データの値に応じで暗号鍵を選択する位置を変更できるようにセレクタを増加させれば良い。また、暗号鍵を64ビット以上にして、４個の32ビット長である変換鍵を生成させ、Ｎ個の換字転置変換手段を２組に分け、２個ずつ供給するような構成にしてもよい。複数個の変換鍵を生成するのに、暗号変換で用いた換字転置変換手段を用いても良い。例えば、8個の32ビット長である変換鍵を生成する鍵変換手段を示す。図８において、鍵変換手段23は、8個の換字転置変換手段211から218と、拡張鍵保持手段100から構成される。拡張鍵保持手段100には、変換鍵を生成するために使用する8個の32ビット長である拡張鍵KE1からKE8が保持されている。64ビットの暗号鍵は、8個の換字転置変換手段211から218を用いて順次変換していく。ここで、各換字転置変換手段の変換アルゴリズムは、アルゴリズム保持手段24に保持されているアルゴリズム鍵により決定される。また、各換字転置変換手段には拡張鍵保持手段100に保持されている拡張鍵が入力される。例えば、換字転置変換手段212には、拡張鍵KE3とKE4が入力される。以上の変換を行っていき、8個の換字転置変換手段211から218の出力値である、L1からL8を8個の変換鍵とする。ここで、拡張鍵保持手段に格納されている変換鍵は、毎回同じ値を用いても良いし、アルゴリズム鍵と同様の方法で更新処理を行ってもよい。さらに、暗号鍵と同様の方法で鍵共有処理を行ってもよい。図８を用いて説明した鍵変換手段23では、暗号変換で用いる換字転置変換手段を共用できるので、例えば本発明に基づいた暗号変換装置をハードウェアで実装した場合、少ない回路規模で、安全性の高い暗号変換を実現することが可能である。次に、本発明による暗号変換装置および復号変換装置の他の実施例を示す。本実施例における暗号変換装置の全体ブロック図は、前記実施例の説明で用いた図２に記載されているものと同様である。図９は、図２の暗号変換部１１内において、n回目の暗号変換を実行する換字転置変換手段21nのブロック図を示す。図９において、換字転置変換手段21nは、ビット列変換部361と、演算部362から構成される。ここで、演算部362では、２つの入力データの排他的論理和演算あるいは加算演算のどちらかを行う。演算部362で、どちらの演算を行うかは、アルゴリズム鍵から決定する。図９における換字転置変換手段21nの変換手順は、前記実施例で説明したものと同様である。図１０は、図９のビット列変換部361のブロック図の一例を示す。ビット列変換部361は、５個のビット列変換器 81から 85で構成される。ビット列変換器 81は、演算部394を備える。ビット列変換器 82は、演算部395と演算部396と循環シフト部91を備える。ビット列変換器 83は、演算部397と演算部398と循環シフト部92を備える。ビット列変換器 84は、演算部399を備える。ビット列変換器 85は、演算部400と演算部401と循環シフト部93を備える。ここで、演算部394から401は、図９における演算部362と同様に、２つの入力データの排他

的論理和演算あるいは加算演算のどちらかを行う。また、どちらの演算を行うかは、アルゴリズム鍵から決定する。ビット列変換部361は、これらのビット列変換関数F1 81からF5 85を変換データに作用させていくことで、ビット列変換を行う。以上のように、本実施例における暗号変換装置は、暗号変換装置内で使用する、加算演算と排他的論理和演算の数を、アルゴリズム鍵から決定することができる。次に、本発明による暗号変換装置および復号変換装置を用いた、他の暗号通信装置の実施例を示す。図１１は、自動料金徴収装置のブロック図を表している。ここで、自動料金徴収装置は、自動車が有料道路を通過する時に、有料道路上に設置されている路側機で、自動車を停止させることなく、運転手のICカードから通行料金を電子決済によって徴収できるシステムである。自動料金徴収装置は、道路の渋滞解消や、ICカードでの電子決済化による利便性の向上など、様々な期待が寄せられている。図１１に示した自動料金徴収装置は、自動車200、路側機201、車載機202、ＩＣカード203、鍵管理機関204で構成される。自動車200には、車載機202が搭載されており、自動車200を運転する時に、ICカード203を車載機202に挿入しておく。路側機201は、有料道路上に設置されており、自動車200が通過する際に、通行料金を徴収する機能を有している。ICカード203には、予め自動料金徴収システムの契約情報が格納されており、自動車200が路側機201を通過する時に、ICカード203が挿入されている車載機202を介した無線通信により、路側機201にこの契約情報を転送し、その後、路側機201から経路情報や決済情報を受信する。これらの処理を安全および正確に行うためには、契約情報、経路情報、および決済情報の正当性の検証と、不正な改竄や盗聴を防止する機能が必要である。したがって、ICカード203と車載機202の間、および車載機202と路側機201の間では、通信相手を正当であると認識するための相手認証処理、交換データの暗号化および復号化のために用いる暗号鍵の共有処理、共有した暗号鍵を用いた暗号通信を行う必要がある。この相手認証処理、鍵共有処理および暗号通信に、本発明に基づいた暗号変換装置および復号変換装置を適用することができる。以上の処理を実現するために、車載機202、ICカード203、および路側機201には、鍵管理組織204が発行した、共通のアルゴリズム鍵と、ライセンス鍵とを事前に保持しておく。例えば製造時に各々の内部に埋め込んでおくことが考えられる。ここで、アルゴリズム鍵の詳細および、アルゴリズム鍵によって定まる暗号変換および復号変換の詳細は前述した通りである。また、ライセンス鍵は、秘密情報として正当な機器に埋め込んでおき、認証処理および鍵共有処理を正しく行うために用いる。例えば、機器Ａと機器Ｂが通信を行うために、機器Ａが正当な機器であることを、機器Ｂが確認する場合を考える。このためには、機器Ａは、自分が保持しているライセンス鍵が正しいことを、機器Bに証明すればよい。ここで、ライセンス鍵は秘密情報であるので、機器Ａは自分のライセンス鍵を明かすことなく、それが正しいことを、機器Ｂに証明しなければならない。この証明は、暗号技術を用いることで実現できる。例えば、対称鍵暗号方式を用いた手法が、セキュリティメカニズムの国際規格であるISO9798-2で説明されている。この対称鍵暗号方式の具体例として、本発明に基づいた暗号変換装置あるいは復号変換装置を適用することができる。次に、図１１を構成するそれぞれの要素について説明する。路側機201は、無線通信部232、暗号復号処理部230、相手認証・鍵共有処理部233、主制御部235、およびデータ保持部234から成る。車載機202は、無線通信部212、暗号復号処理部210、ＩＣカード通信部211、相手認証・鍵共有処理部213、データ保持部214および主制御部215から成る。ＩＣカード203は、ＩＣカード通信部221、暗号復号処理部220、 相手認証・鍵共有処理部223、データ保持部224、および主制御部225から成る。ここで、暗号復号変換処理部210、220、および230は、前述した、本発明に基づく、暗号変換装置および復号変換装置を内蔵しており、データの暗号化および復号化を行うことが可能である。また、ICカード通信部211および221は、車載機202とＩＣカード203の間の通信処理を行うために用いられる。さらに、無線通信部212および232は、車載機202と路側機201の間の無線通信処理を行うために用いられる。さらに、認証・鍵共有処理部213、223、および233は、通信相手を正当であると認識するために行う認証処理、およびデータの暗号化および復号化のために用いる暗号鍵の共有処理を行う。認証・鍵共有処理部213は、認証処理および鍵共有処理を行うために、暗号復号処理部210が提供する暗号変換機能および復号変換機能を用いる。同様の機能を実現するために、認証・鍵共有処理部223は、暗号復号変換処理部220を用いる。同様に、認証・鍵共有処理部233は、暗号復号変換処理部230を用いる。データ保持部214、224、および234には、鍵管理機関204から取得した、アルゴリズム鍵、およびライセンス鍵を保持しておくのに用いる。また、契約情報、経路情報および決済情報も保持できるのもとする。図１２は、図１１の自動料金徴収装置の通信フロー図を示す。図１２のフロー図では、まず、図１１のＩＣカード203を車載機202に設定した時点で、ＩＣカード203と車載機202の間で、相手認証・鍵共有処理240が行われる。そして、相手認証・鍵共有処理240が成功した後に、ＩＣカード203は、契約情報を車載機202に転送するために、暗号通信241を行う。車載機202は、ＩＣカード203の契約情報を取得すると、車載機202内のデータ保持部214（図１１）で秘密に保持しておく。次に、図１１の自動車200が路側機201を通過する時点で、車載機202と路側機201の間で、相手認証・鍵共有処理250が行われる。そして、相手認証・鍵共有処理250が成功した後に、車載機202は、先にICカードから取得

した契約情報を、路側機201に転送するために、暗号通信251を行う。この暗号通信251は、路側機201から車載機202に、経路情報および決済情報を転送するためにも用いられる。次に、車載機202は、路側機201から得た経路情報と決済情報をＩＣカード203に転送するために、暗号通信261を行う。ここで、道路通行料金の決済はICカード203と路側機201との間で行われるが、ICｶｰﾄﾞ203と路側機201とは、車載機202を介さないと通信が行えない。この場合、車載機202が不正処理を行うことで、不正な決済が行われてしまう可能性も考えられる。このような事態が発生した場合に備えて、路側機201は、ICカード203との決済で用いた車載機202を特定できるようにしておく必要がある。たとえば、車載機202に識別番号を割り当て、車載機202は、ICカード203との相手認証・鍵共有処理240の中で、車載機202の識別番号をICカード203に転送するようにする。ICカード203は、車載機202の識別番号とICカード203の決済履歴の両方に対する、デジタル署名を生成して返送する。そして、車載機202は、自分の識別番号と、ICカード203から取得したデジタル署名を、路側機201に、相手認証・鍵共有処理250の中で転送するようにする。その後、路側機201は、ICカード203が生成したデジタル署名を検証することで、車載機202が、いつ用いられたかを特定することが可能になる。また、暗号通信241、251および261において、通信路上を流れる暗号化データを第三者に改竄されないようにしておく必要がある。これを実現するためには、受信したメッセージが正当であることを判定できる、メッセージ認証を行う必要がある。メッセージ認証を行うためには、送信者と受信者が予めメッセージ認証鍵を秘密に共有しておく。メッセージ認証鍵の共有は、例えば図１２に記した、相手認証・鍵共有処理250内で行う。そして、送信者が、転送するメッセージとメッセージ認証鍵から、メッセージ認証子（MAC: Message Authentication Code）と呼ばれるデータを生成する。送信者は、メッセージと一緒にメッセージ認証子を、受信者に転送する。受信者は、受信したメッセージ認証子を、メッセージ認証鍵を用いて検証する。この検証によって、受信したメッセージが改竄されているかどうかを判定できる。メッセージ認証に関しては、例えば、対称鍵暗号方式を用いた手法が、セキュリティメカニズムの国際規格であるISO9797で説明されている。この対称鍵暗号方式の具体例として、本発明に基づいた暗号変換装置あるいは復号変換装置を適用することができる。図１３は、メッセージ認証を含んだ暗号通信の例として、暗号通信241の詳細フロー図を示す。図１３のフロー図では、まずICカード203が、メッセージ認証子の生成を、MAC生成処理261で行う。次に、転送メッセージとメッセージ認証子を結合する、結合処理262を行う。その後、転送メッセージとメッセージ認証子を結合したデータを暗号化する暗号処理263が行われ、暗号化データが生成される。次に、車載機202が、暗号化データを受信し、まず復号化処理264を行う。その後、分離処理265を行うことで、ICカードが転送した、メッセージとメッセージ認証子を復元する。次に、復元されたメッセージ認証子を検証する、MAC検証処理266を行い、受信したメッセージの正当性を検証する。これによって、課金情報や経路情報などの盗聴や改竄されてはならないデータを安全に交換することが可能になる。以上の処理を行うことにより、通行料金をＩＣカード203内に課金し、さらに路側機201で課金情報を管理することができる。

【発明の効果】本発明によれば、暗号変換のアルゴリズムを可変にし、使用するアルゴリズムを第三者から隠すことで、暗号解読に強い、高速な暗号変換装置、復号変換装置、暗号通信装置および自動料金徴収装置を実現することができる。

【図面の簡単な説明】

【図１】本発明における、送信機器と受信機器とが行う暗号通信装置の一実施例である。

【図２】図１における、暗号変換部を示すブロック図である。

【図３】図２における、鍵変換手段のブロック図である。

【図４】図２における、換字転置変換手段のブロック図である。

【図５】図４における、ビット列変換部のブロック図である。

【図６】図１における、復号変換部を示すブロック図である。

【図７】図６における、換字転置変換手段の一実施例のブロック図である。

【図８】本発明における、鍵変換手段のブロック図の例である。

【図９】本発明における、換字転置変換手段の他の実施例のブロック図である。

【図１０】本発明における、ビット列変換部の他の実施例のブロック図である。

【図１１】本発明における、暗号通信の他の実施例であり、自動料金徴収装置の構成図である。

【図１２】本発明における、自動料金徴収装置の通信フローを示す図である。

【図１３】本発明における、自動料金徴収装置で用いる暗号通信を示す図である。

【符号の説明】

1　データ送信機器
2　データ受信機器
3　鍵管理機関
11　暗号変換部
12　鍵共有部
13　データ処理部
14　通信処理部

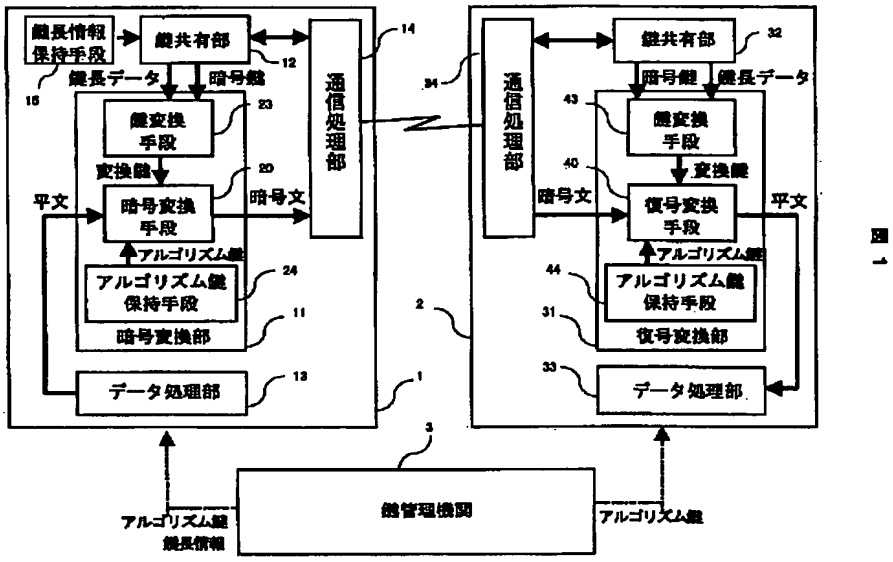
17

15　鍵著データ保持手段
20　暗号変換手段
211～21N　換字転置変換手段
23　鍵変換手段
24　アルゴリズム鍵保持手段
31　復号変換部
32　鍵共有部

18

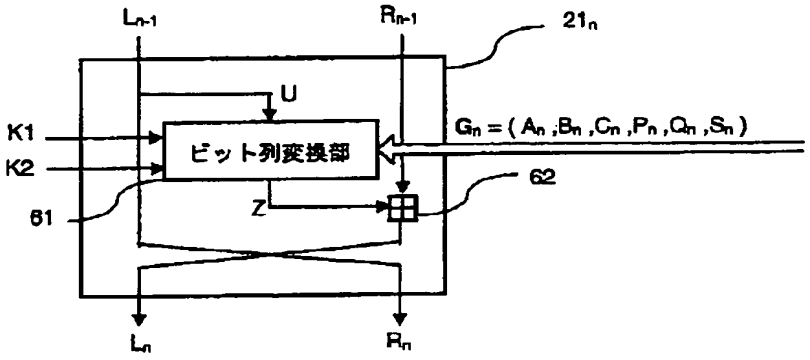
33　データ処理部
34　通信処理部
411～41N　換字転置変換手段
43　鍵変換手段
44　アルゴリズム鍵保持手段
81　鍵送信部
82　鍵受信部

【図１】



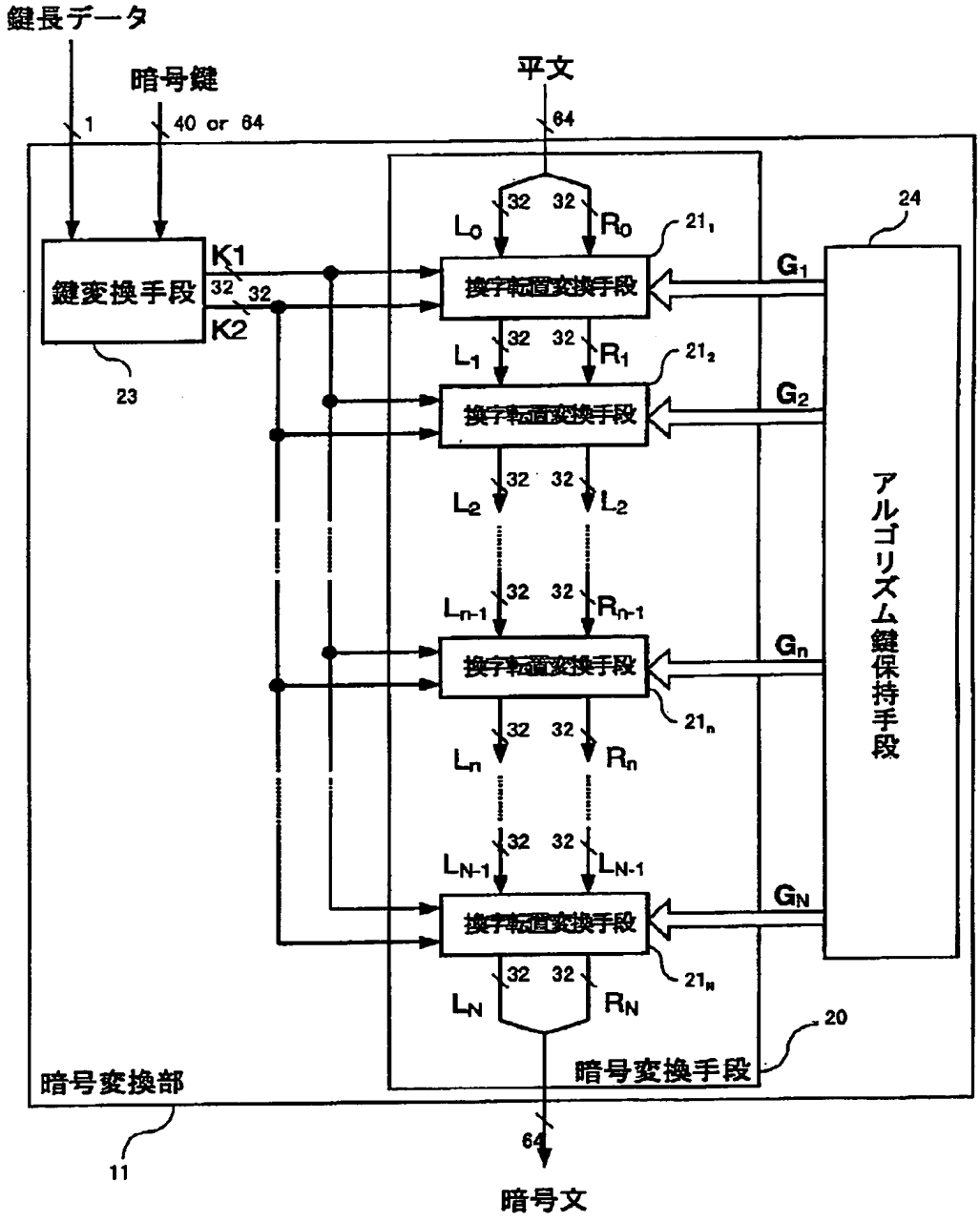
【図４】

図４



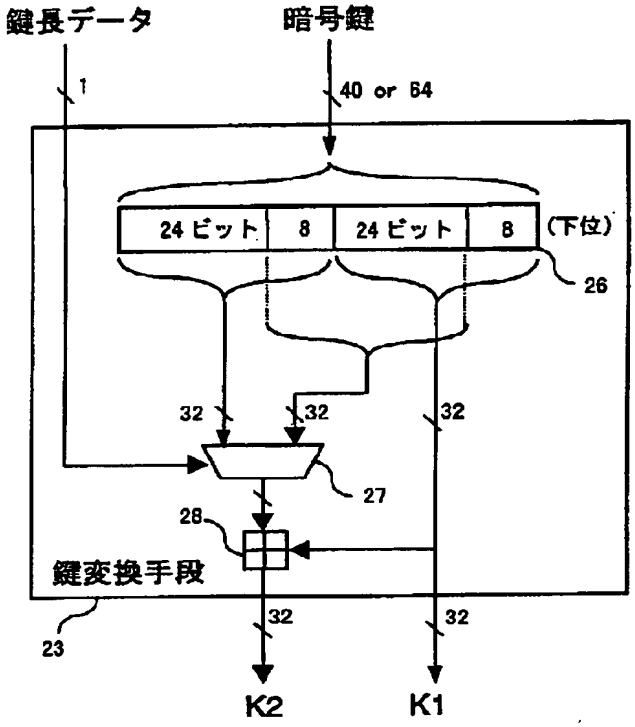
【図２】

図２


鍵長データ
暗号鍵
1
40 or 64
平文
64
鍵変換手段
K1
K2
32
32
23
L0
R0
21₁
換字転置変換手段
G1
24
L1
R1
21₂
G2
L2
L2
アルゴリズム鍵保持手段
Ln-1
Rn-1
Gn
21n
Ln
Rn
LN-1
LN-1
GN
21N
LN
RN
20
暗号変換手段
暗号変換部
11
64
暗号文

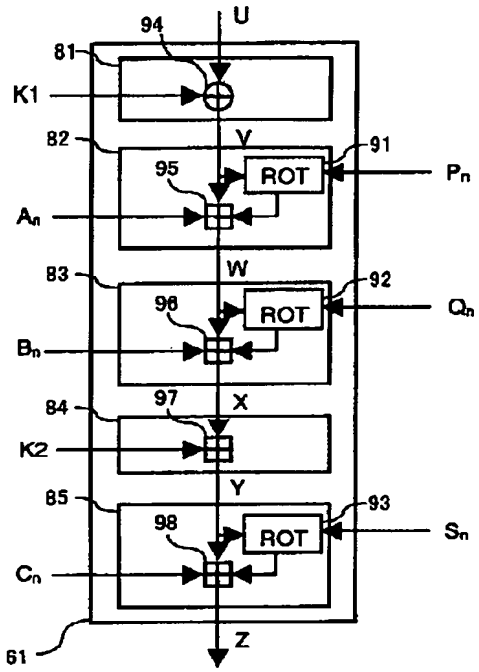
【図３】

図３



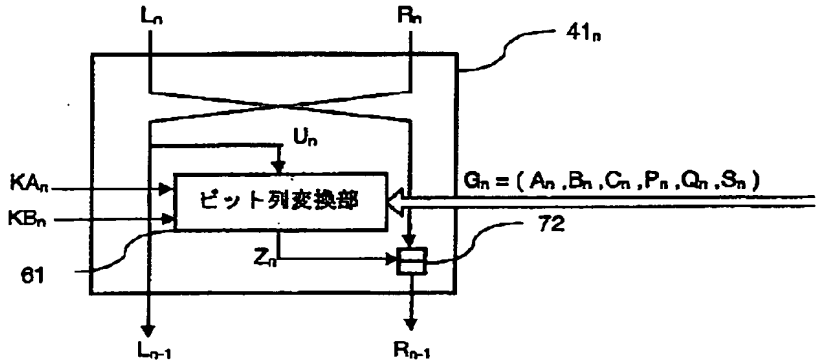
【図５】

図５



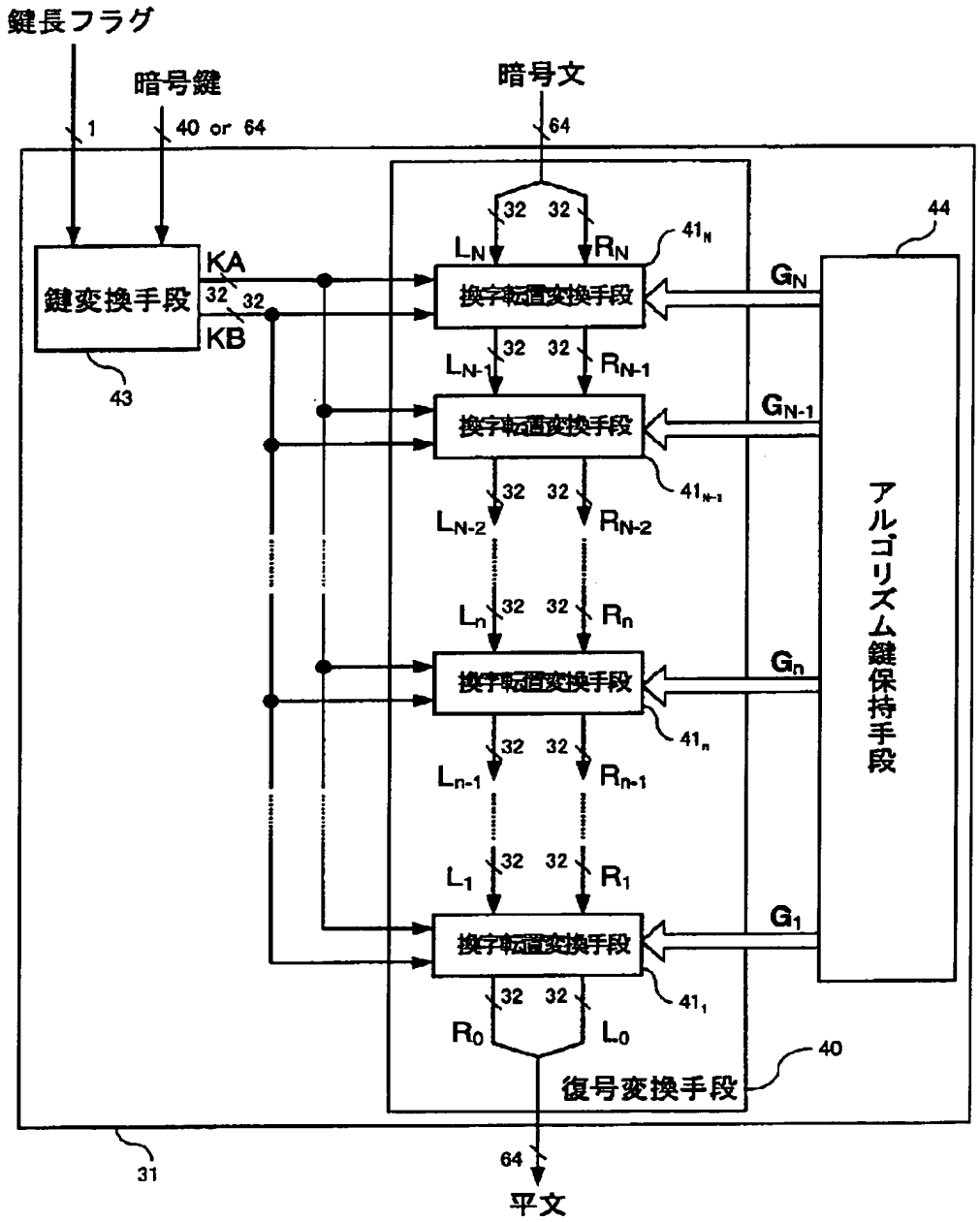
【図７】

図７



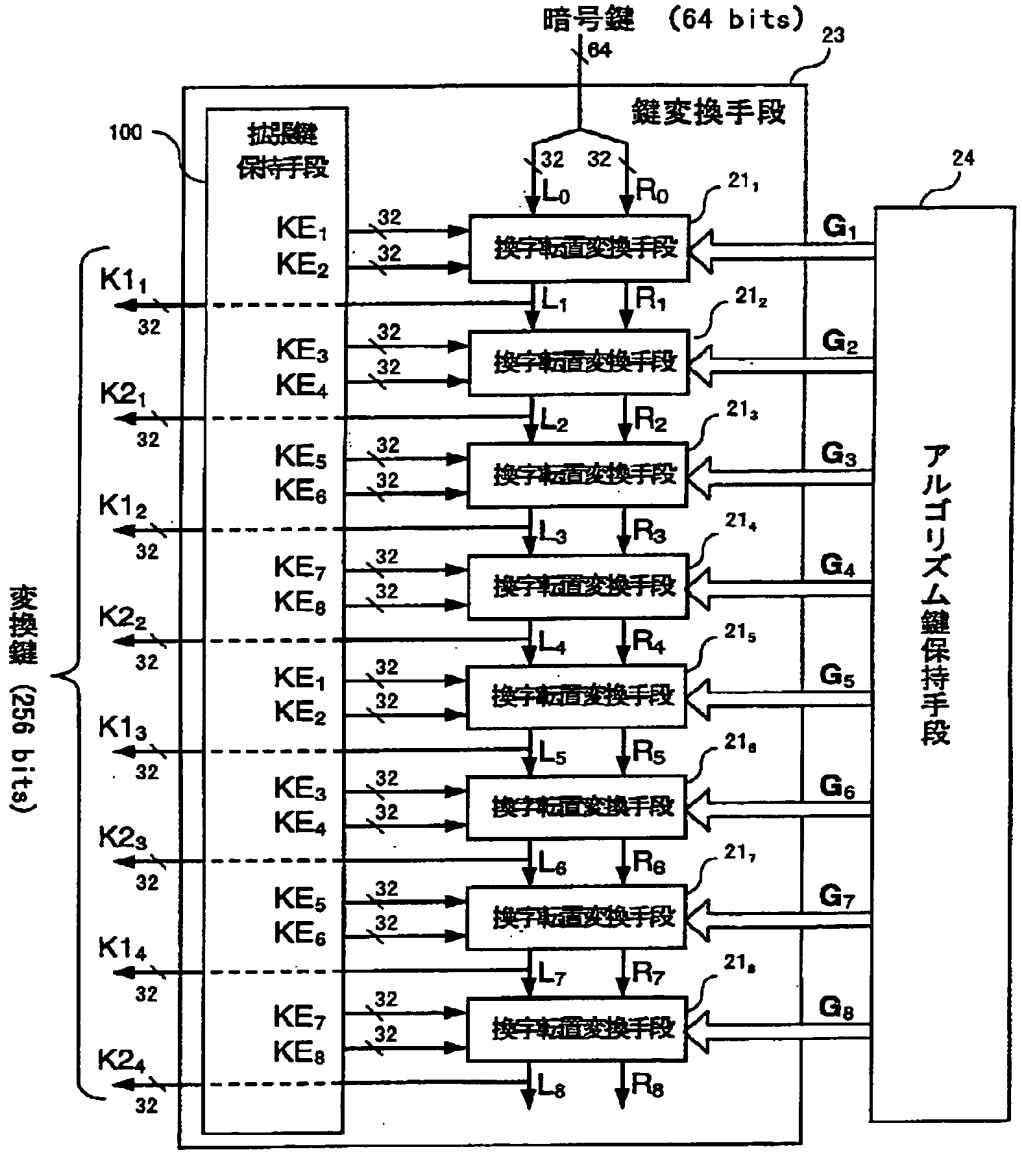
【図６】

図６


鍵長フラグ
暗号鍵
暗号文
1
40 or 64
64
鍵変換手段
KA
KB
32
43
換字転置変換手段
L_N
R_N
41_N
G_N
L_{N-1}
R_{N-1}
G_{N-1}
41_{N-1}
L_{N-2}
R_{N-2}
L_n
R_n
G_n
41_n
L_{n-1}
R_{n-1}
L_1
R_1
G_1
41_1
R_0
L_0
44
アルゴリズム鍵保持手段
40
復号変換手段
31
64
平文

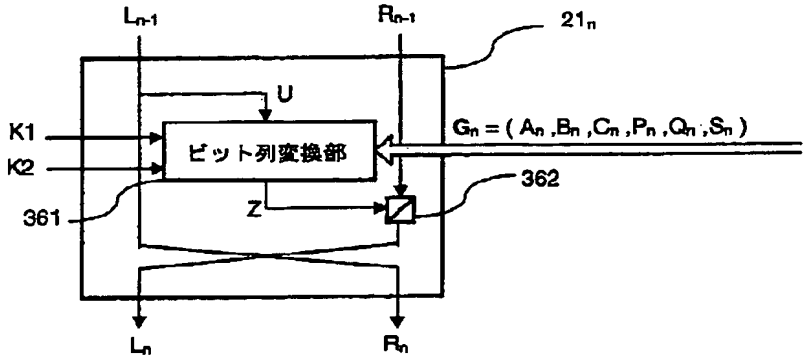
【図８】

図８


暗号鍵 (64 bits)
64
23
鍵変換手段
100
拡張鍵保持手段
32 32
L0 R0
21₁
24
KE1 KE2
32 32
換字転置変換手段
G1
K11
32
L1 R1
21₂
KE3 KE4
G2
K21
L2 R2
21₃
KE5 KE6
G3
K12
L3 R3
21₄
KE7 KE8
G4
K22
L4 R4
21₅
KE1 KE2
G5
K13
L5 R5
21₆
KE3 KE4
G6
K23
L6 R6
21₇
KE5 KE6
G7
K14
L7 R7
21₈
KE7 KE8
G8
K24
L8 R8
変換鍵 (256 bits)
アルゴリズム鍵保持手段

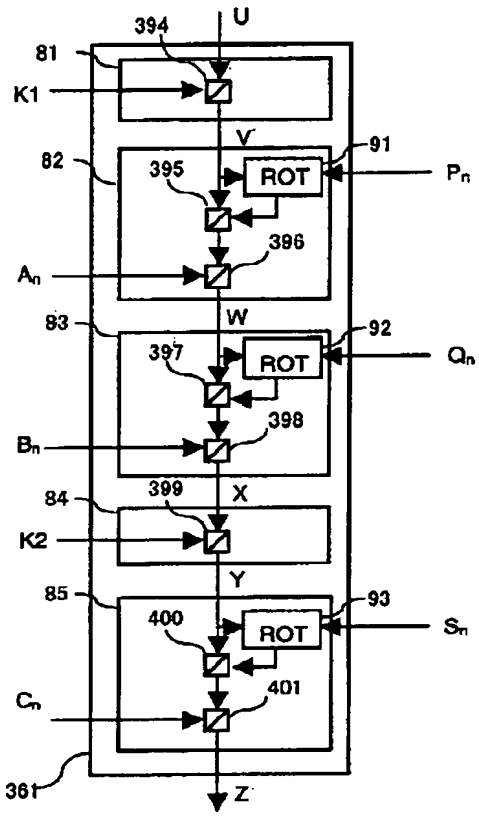
【図９】

図９


L_{n-1}
R_{n-1}
21_n
U
K1
K2
ビット列変換部
$G_n = (A_n, B_n, C_n, P_n, Q_n, S_n)$
361
Z
362
L_n
R_n

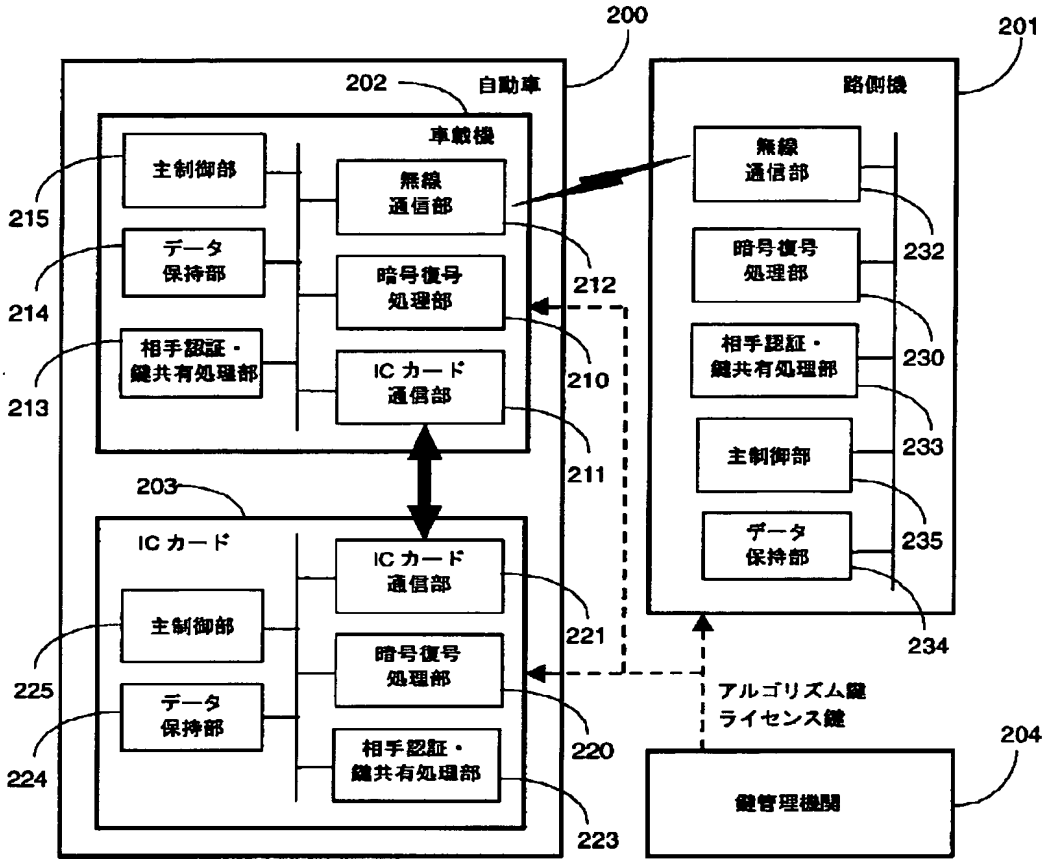
【図１０】

図１０


U
394
81
K1
V
91
82
395
ROT
P_n
396
A_n
W
83
92
397
ROT
Q_n
398
B_n
399
X
84
K2
Y
85
93
400
ROT
S_n
401
C_n
361
Z

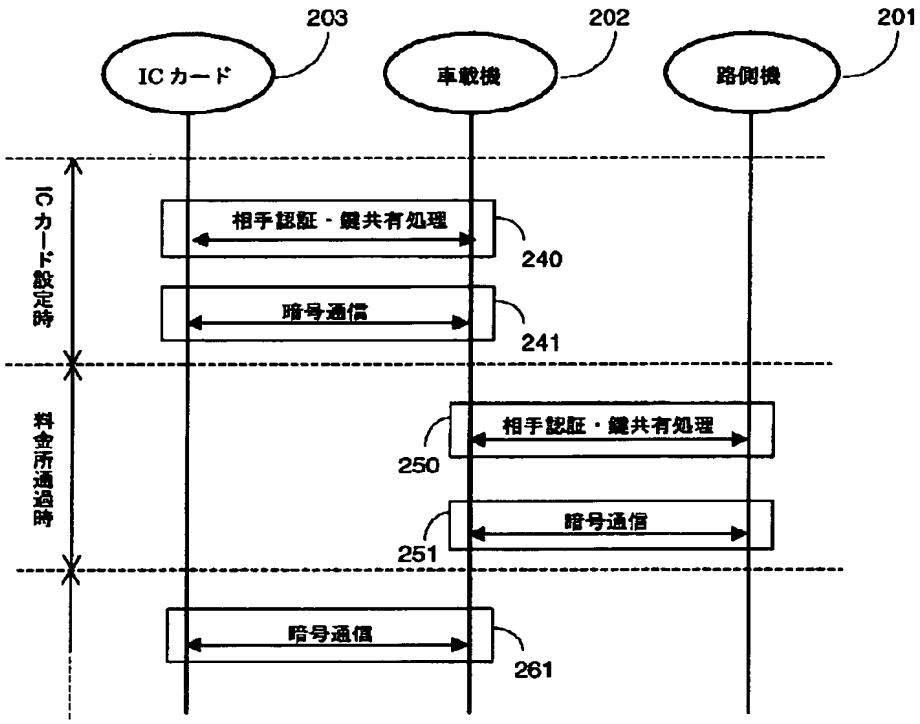
【図１１】

図 １１


200
201
202
自動車
路側機
車載機
主制御部
無線
通信部
データ
保持部
暗号復号
処理部
相手認証・
鍵共有処理部
IC カード
通信部
215
214
213
212
210
211
203
IC カード
主制御部
データ
保持部
IC カード
通信部
暗号復号
処理部
相手認証・
鍵共有処理部
225
224
221
220
223
無線
通信部
暗号復号
処理部
相手認証・
鍵共有処理部
主制御部
データ
保持部
232
230
233
235
234
アルゴリズム鍵
ライセンス鍵
204
鍵管理機関

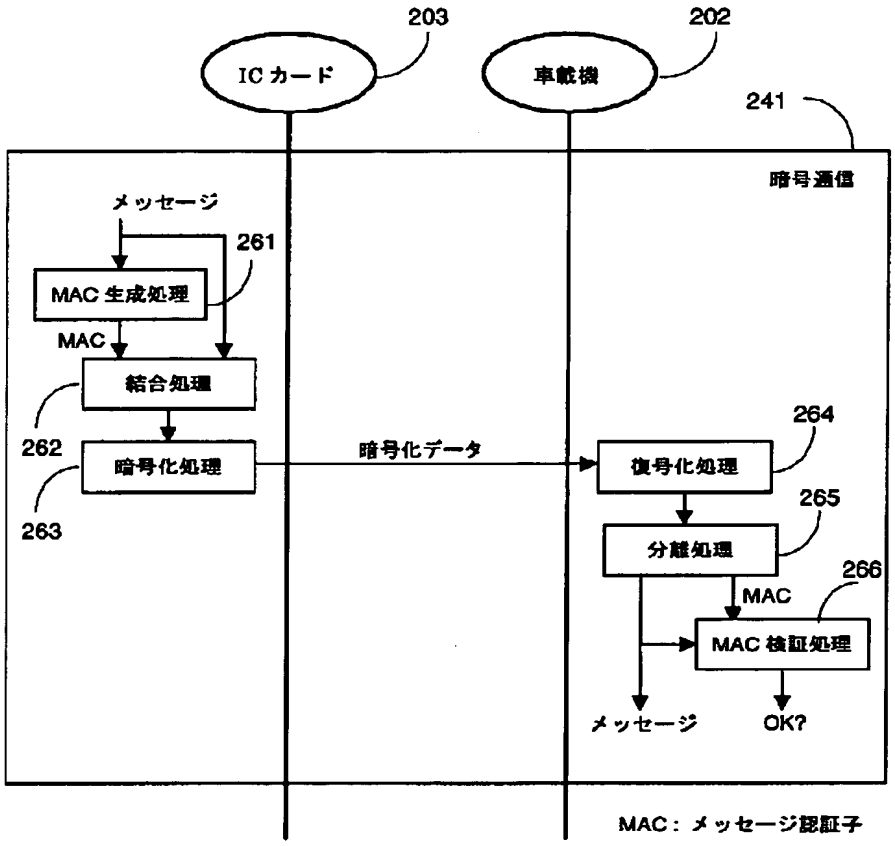
【図１２】

図１２


203
202
201
ICカード
車載機
路側機
ICカード設定時
相手認証・鍵共有処理
240
暗号通信
241
料金所通過時
相手認証・鍵共有処理
250
暗号通信
251
暗号通信
261

【図１３】

図１３



フロントページの続き

(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　工藤　善道
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内